Case Study: Digital Care Planning System Transition — When Implementation Becomes a Governance Risk

Background

PGQ Solutions recently supported providers who had moved from one digital care planning system to another. The intention behind the transition was positive: to modernise care records, improve oversight, increase accessibility of information and strengthen governance.

However, during review work undertaken by Lisa and Kelly, it became clear that the transition had not been supported by a sufficiently robust rollout and implementation plan. While the new system had been introduced, the provider had not fully assured itself that essential care information had transferred accurately, that staff understood how to use the new system effectively, or that managers had reliable oversight of the risks created during the change.

This created avoidable operational, clinical and regulatory risk.

The issue was not the digital system itself. The risk came from the way the transition had been planned, implemented, checked and embedded.

The presenting concern

Following the migration, staff were expected to use the new digital care planning system as the primary record for people's care and support. However, staff confidence and competency varied significantly.

Some staff were unsure where to record key information. Others were unclear where to locate important care plan detail, risk assessments, professional guidance or daily monitoring records. Managers believed that information had transferred, but there was limited evidence of a structured post-migration audit to confirm that care plans remained accurate, complete and person-centred.

This meant that the provider was exposed to risk in several areas:

- important care plan detail may not have been transferred in full;
- risk assessments may not have reflected the person's current needs;
- staff may not have had immediate access to essential information;
- care delivery could become inconsistent;
- oversight of clinical and operational risk was weakened;

- governance assurance was based on assumption rather than evidence.

Key risks identified

The review identified several areas where digital migration can create risk if it is not managed through a clear governance framework.

1. Loss of important care plan detail

When information is transferred from one system to another, there is a risk that important narrative detail is lost. This can include personal preferences, communication needs, behaviours of concern, distress triggers, family involvement, clinical history, routines, meaningful activity, cultural needs and person-centred guidance.

In adult social care, this information is not supplementary. It is often the information that enables staff to provide safe, consistent and personalised support.

2. Risk assessments not transferring accurately

Risk assessments relating to falls, choking, nutrition, hydration, skin integrity, mobility, medication, behaviours, mental capacity, safeguarding and environmental risks must remain accurate and accessible throughout any system change.

Where these are incomplete, out of date or difficult for staff to locate, the provider may be unable to demonstrate that risks are being properly assessed, monitored and mitigated.

3. Staff training focused on navigation rather than safe use

Training on a new digital system must go beyond showing staff how to log in and where to click.

Staff need to understand how the system supports safe care. They should know where to find critical information, how to record changes, how to escalate concerns, how to update daily records, and how to ensure that care delivery reflects the person's current needs.

Where staff training is insufficient, the provider may have a digital system in place but still have unsafe or inconsistent recording practice.

4. Weak post-implementation assurance

A common risk is that providers assume the migration has been successful because the new system is live.

However, going live is not the same as being embedded.

Providers need to test whether the system is working in practice. This should include post-migration audits, staff knowledge checks, care plan sampling, manager walkarounds, review of daily notes, and checks that high-risk information is visible and understood.

5. Regulatory exposure

Digital care planning system transitions can create regulatory risk across several CQC key questions, including Safe, Effective, Responsive and Well-led.

If inspectors ask how the provider assured itself that care records remained accurate during migration, the provider should be able to show a clear plan, audit trail, staff training records, risk review, action plan and evidence of management oversight.

Without this, the provider may struggle to demonstrate good governance.

Why this matters

A digital care planning system is only as effective as the information within it and the staff using it.

A provider may invest in a strong digital platform, but if the implementation is poorly planned, it can create a false sense of assurance. Leaders may believe they have improved oversight, when in reality staff are unsure, records are incomplete, and key care information is fragmented.

For people receiving care, this can mean that important details about their needs, preferences and risks are not consistently understood. For providers, it can mean increased regulatory exposure, weaker evidence, reduced confidence in care records and greater difficulty demonstrating safe, person-centred care.

What good should look like

A safe digital care planning system transition should be treated as a formal governance project, not simply an IT change.

Providers should be able to evidence:

- a clear implementation and rollout plan;
- named leads responsible for the transition;
- pre-migration review of existing care plan quality;
- data mapping between the old and new systems;
- identification of high-risk records;
- clinical and operational sign-off;

- staff training records;
- competency checks;
- super-user or champion support;
- contingency plans;
- post-migration audits;
- action plans where gaps are identified;
- registered manager and provider oversight;
- evidence that the system is embedded in day-to-day practice.

The strongest providers do not simply ask, “Has the system gone live?”

They ask:

Has the information transferred accurately?
Can staff find what they need?
Are risks visible?
Are records person-centred?
Is the manager assured?
Can the provider evidence safe implementation?
Has the change improved outcomes for people?

How PGQ Solutions supported the provider

PGQ Solutions approached the issue through a governance, regulatory and operational lens.

The review considered whether the provider could demonstrate that the digital transition had been safely implemented and whether the new system was supporting effective care delivery.

Support included:

- reviewing care plan content following migration;
- identifying gaps in transferred information;
- checking whether key risks were visible and current;
- reviewing staff understanding of the new system;
- considering whether training had been sufficient;
- assessing management oversight and audit activity;
- identifying regulatory risks;

- supporting the provider to develop a clear improvement plan;
- advising on evidence required to demonstrate safer implementation;
- strengthening governance around digital records.

The focus was not to criticise the use of digital systems. Digital care planning can significantly improve care, oversight and accountability. The focus was to ensure that implementation was safe, structured and evidenced.

Key learning for providers

Digital transformation must be led through governance.

Before changing systems, providers should consider whether they have the right people, plan, training, audit process and assurance framework in place.

The key learning from this case study is clear:

Digital change without governance creates risk.
Digital change with clear oversight can strengthen safety, quality and compliance.

Providers should not assume that a new system automatically improves care. They must be able to evidence that the system is accurate, embedded, understood by staff and improving outcomes for people.

How PGQ Solutions can help

PGQ Solutions supports providers before, during and after digital care planning system transitions.

Our support can include:

- pre-migration care plan quality reviews;
- digital transition risk assessments;
- implementation plan review;
- data migration audits;
- staff knowledge and competency checks;
- post-migration care record sampling;
- regulatory risk reviews;
- action plan development;
- governance meeting support;
- evidence mapping against CQC expectations;

- provider assurance reporting.

We help providers identify risk early, strengthen implementation, protect important care information and demonstrate that digital systems are supporting safe, effective and person-centred care.